SAP Community

Ask a Question Write a Blog Post Login

Alessandro Banzer

February 23, 2014 | 2 minute read

Risk Lifecycle

2 8 11,841

Follow

Like

RSS Feed

A high amount of time during a SAP GRC project will be spent on defining processes and responsibilities. My suggestion is to think in lifecycles for getting a better understanding of the processes and who is taking over the responsibilty.

In this post I would like to clarify the lifecycle of Risks. I have grouped them into four steps Create, Change, Delete and Review. Please see for each step expected Tasks and who is involved.

On request I have additionally added the RACI matrix to see who is **R**esponsible, **A**ccountable,**C**onsulted and **I**nformed for each step. Please be aware that this is very much depending on the point of view and can be different in your organization. My considerations are commonsense and pretty much of thinking in smooth processes throughout a global enterprise.

Creation of Risks

Tasks

- Define the SoD risk on business level (e.g. with internal auditors)
- Evaluate the necessary transactions to execute the SoD conflict (transaction and authorization)

- Implement the risk within SAP GRC AC
- Validate the risk analysis results

Involved functions

- Risk owner
- Process owner
- ICS responsible
- SAP GRC responsible

Creation of Risks	Risk owner	Process owner	Internal Contrd responsible	SAP GRC responsible
Define the SoD Risk on business level	A	A	R	
Evaluate the necessary transaction to execute the SoD conflict	R	C	A	C
Implement the risk withing SAP GRC AC	A	I	I	R
Valiate the risk analysis results	R	I	A	C

Changing of Risks

Tasks

- Define the changes within the SoD risk on business level (e.g. with internal auditors)
- Evaluate the necessary transactions to execute the SoD conflict (transaction and authorization)
- Change the risk within SAP GRC AC
- Validate the risk analysis results

Involved functions

- Risk owner
- Process owner
- ICS responsible
- SAP GRC responsible

Changing of Risks	Risk owner	Process owner	Internal Contrd responsible	SAP GRC responsible
Define the changes within the SoD Risk on business level	A	A	R	
Evaluate the necessary transaction to execute the SoD conflict	R	C	A	C
Change the risk withing SAP GRC AC	A	I	I	R
Valiate the risk analysis results	R	I	A	C

Deletion of Mitigation Controls

Tasks

- Delete risks within SAP GRC AC which are not valid anylonger
- Document the deletion of the risk and especially the decision to delete the risk

Involved functions

- Risk owner
- ICS responsible
- SAP GRC responsible

Deletion of Risks	Risk owner	Internal Contrd responsible	SAP GRC responsible
Delete risks withing SAP GRC AC	A	A	R
Document the deletion of the risk	C	R	I

Reviewing of Risks

Tasks

- Analyse if maintained risks within SAP GRC are still valid
- Define actions to take because of:
  - New business processes
  - Changes in the IT system
  - Changes in the Internal Control System

Involved functions

- Risk owner
- Process owner
- ICS responsible
- SAP GRC responsible

Reviewing of Risks	Risk owner	Process owner	Internal Control responsible	SAP GRC responsible
Analyse if maintained risks are still valid	R	C	A	
Define actions based on new business processes	C	R	A	I
Define actions based on changes in the IT system	A	C	R	I
Define actions based on changes in the Internal Control System	A	C	R	I

If you want to have further information or contribute in this blog post do not hesitate to contact me directly.

Alert Moderator

Assigned Tags

SAP Access Control

governance risk and compliance sap grc

grc

risks

Similar Blog Posts

ARA - For the new kid on the block

By S A Aug 27, 2014

SAP IAG Bridge – Manage Hybrid Landscapes

By Alessandro Banzer Jun 29, 2021

Firefighter ID Lifecycle

By Alessandro Banzer Mar 03, 2014